

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2002-259606

(P 2002-259606A)

(43) 公開日 平成14年9月13日 (2002.9.13)

(51) Int. Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 F 17/60	1 4 2 3 0 2 3 4 0 5 0 4	G 0 6 F 17/60 1 4 2 3 0 2 E 3 4 0 5 0 4 9/06 6 6 0 C	5B076
1/00			
審査請求 未請求 請求項の数 18	OL		(全 13 頁)

(21) 出願番号 特願2001-55976 (P2001-55976)

(22) 出願日 平成13年2月28日 (2001.2.28)

(71) 出願人 390009531

インターナショナル・ビジネス・マシー
ズ・コーポレーション

INTERNATIONAL BUSIN
ESS MASCHINES CORPO
RATION

アメリカ合衆国10504、ニューヨーク州

アーモンク ニュー オーチャード ロ
ード

(74) 復代理人 100112520

弁理士 林 茂則 (外2名)

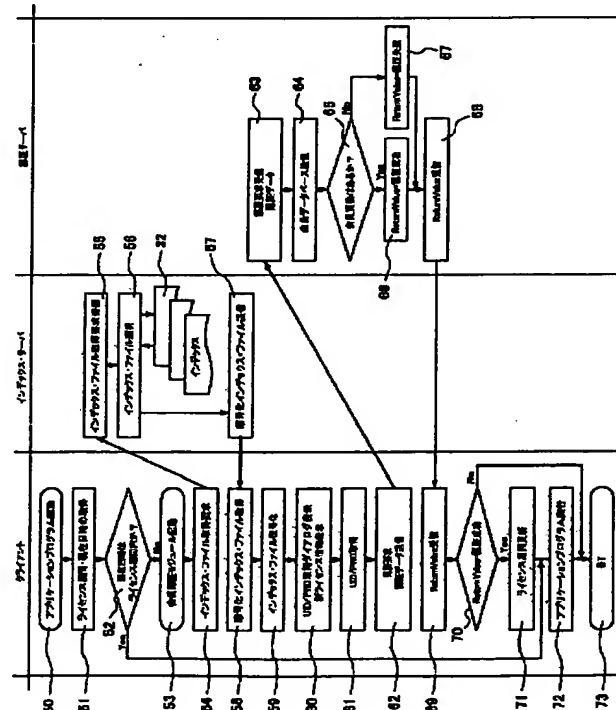
最終頁に続く

(54) 【発明の名称】 プログラム使用許諾期間の更新方法、プログラムの使用許諾方法、情報処理システムおよびプログラ
ム

(57) 【要約】

【課題】 プログラム使用許諾 (ライセンス) 期間の更
新を自動的に行う。

【解決手段】 現在日時がプログラムの使用許諾期間内
であるかを判断し (ステップ52)、インデックス・サ
ーバにインデックス・ファイルの送信要求を発生 (ス
テップ54)、インデックス・サーバからインデックス・
ファイルを受信し (ステップ58)、インデックス・フ
ァイルに含まれる認証サーバのアドレスに、認証要求を
発生 (ステップ62)、認証サーバから認証情報を受信
し (ステップ69)、認証成功の場合にはプログラムの
使用許諾期間を更新し (ステップ71)。プログラムを
実行する (ステップ72)。



【特許請求の範囲】

【請求項 1】 現在日時がプログラムの使用許諾期間内であるかを判断する第 1 判断ステップと、
前記第 1 判断ステップの前記判断が偽の場合、インデックス・サーバに対し、インデックス・ファイルの送信要求を発するステップと、
前記インデックス・サーバからインデックス・ファイルを受信するステップと、
前記インデックス・ファイルに含まれる認証サーバのアドレスに、認証要求を発するステップと、
前記認証サーバから認証情報を受信するステップと、
前記認証情報に認証成功の情報が含まれるかを判断する第 2 判断ステップと、
前記第 2 判断ステップの前記判断が真の場合、前記プログラムの使用許諾期間を更新するステップと、
を含むプログラム使用許諾期間の更新方法。

【請求項 2】 前記第 1 判断ステップは、前記プログラムの起動を契機として実行され、
前記使用許諾期間の更新の後に前記プログラムの実行が可能になる請求項 1 記載の方法。

【請求項 3】 前記インデックス・ファイルに含まれる前記認証サーバのアドレス情報が暗号化されており、
前記暗号化された前記認証サーバのアドレス情報を復号化するステップをさらに有する請求項 1 記載の方法。

【請求項 4】 前記認証要求には、前記プログラムの使用が許諾されているグループに属するか否かを判断するためのユーザ識別情報を含み、
前記認証サーバは、前記グループを管轄する者が管理するものである請求項 1 記載の方法。

【請求項 5】 前記認証要求を発する前に、前記ユーザ識別情報とパスワードとを入力するよう要求する画面を表示するステップをさらに有する請求項 4 記載の方法。

【請求項 6】 前記インデックス・ファイルには前記プログラムの使用許諾条件に関する情報が含まれており、
前記画面には、前記ユーザ識別情報とパスワードの入力要求に加えて前記プログラムの使用許諾条件に関する情報を表示する請求項 5 記載の方法。

【請求項 7】 ユーザからの要求を受取るステップと、
前記要求の受信を契機として、前記ユーザが使用するプログラムの使用許諾に関する認証を与えるサーバのアドレス情報を含むインデックス・ファイルを生成または選択するステップと、
前記インデックス・ファイルを前記要求を発したユーザに送信するステップと、
を有するプログラムの使用許諾方法。

【請求項 8】 前記インデックス・ファイルに含まれる前記アドレス情報の部分は暗号化される請求項 7 記載の方法。

【請求項 9】 現在日時がプログラムの使用許諾期間内であるかを判断する第 1 判断手段と、

前記第 1 判断手段の前記判断が偽の場合、インデックス・サーバに対し、インデックス・ファイルの送信要求を発する手段と、

前記インデックス・サーバからインデックス・ファイルを受信する手段と、

前記インデックス・ファイルに含まれる認証サーバのアドレスに、認証要求を発する手段と、

前記認証サーバから認証情報を受信する手段と、

前記認証情報に認証成功の情報が含まれるかを判断する第 2 判断手段と、

10 前記第 2 判断手段の前記判断が真の場合、前記プログラムの使用許諾期間を更新する手段と、
を含む情報処理システム。

【請求項 10】 前記第 1 判断手段は、前記プログラムの起動を契機として実行され、
前記使用許諾期間の更新の後に前記プログラムが実行可能になる請求項 9 記載のシステム。

【請求項 11】 前記インデックス・ファイルに含まれる前記認証サーバのアドレス情報が暗号化されており、
20 前記暗号化された前記認証サーバのアドレス情報を復号化する手段をさらに有する請求項 9 記載のシステム。

【請求項 12】 前記認証要求には、前記プログラムの使用が許諾されているグループに属するか否かを判断するためのユーザ識別情報を含み、
前記認証サーバは、前記グループを管轄する者が管理するものである請求項 9 記載のシステム。

【請求項 13】 前記ユーザ識別情報とパスワードとを入力するよう要求する画面を表示する手段をさらに有する請求項 12 記載のシステム。

【請求項 14】 前記インデックス・ファイルには前記プログラムの使用許諾条件に関する情報が含まれており、

前記画面には、前記ユーザ識別情報とパスワードの入力要求に加えて前記プログラムの使用許諾条件に関する情報を表示する請求項 13 記載のシステム。

【請求項 15】 ユーザからの要求を受取る手段と、
前記要求の受信を契機として、前記ユーザが使用するプログラムの使用許諾に関する認証を与えるサーバのアドレス情報を含むインデックス・ファイルを生成または選
40 択する手段と、

前記インデックス・ファイルを前記要求を発したユーザに送信する手段と、を有する情報処理システム。

【請求項 16】 前記インデックス・ファイルに含まれる前記アドレス情報の部分を暗号化する手段をさらに有する請求項 15 記載のシステム。

【請求項 17】 現在日時がプログラムの使用許諾期間内であるかを判断する第 1 判断機能と、
前記第 1 判断機能の前記判断が偽の場合、インデックス・サーバに対し、インデックス・ファイルの送信要求を発する機能と、

前記インデックス・サーバからインデックス・ファイルを受信する機能と、
 前記インデックス・ファイルに含まれる認証サーバのアドレスに、認証要求を発する機能と、
 前記認証サーバから認証情報を受信する機能と、
 前記認証情報に認証成功の情報が含まれるかを判断する第2判断機能と、
 前記第2判断機能の前記判断が真の場合、前記プログラムの使用許諾期間を更新する機能と、
 をコンピュータに実現させるためのプログラム。
【請求項18】 ユーザからの要求を受取る機能と、
 前記要求の受信を契機として、前記ユーザが使用するプログラムの使用許諾に関する認証を与えるサーバのアドレス情報を含むインデックス・ファイルを生成または選択する機能と、
 前記インデックス・ファイルを前記要求を発したユーザに送信する機能と、
 をコンピュータに実現させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、プログラムの使用許諾期間（ライセンス期間）の更新方法、情報処理システムおよびプログラムに関する。特に、ライセンス期間が満了した場合のライセンス更新を簡略化し、ユーザに煩雑な手続を強いることのないライセンス更新に適用して有効な技術に関する。

【0002】

【従来の技術】 コンピュータ・プログラムは著作権で保護されるため、著作権フリーないわゆるフリーウェアを除き、ライセンス方式によってその使用が許諾されるのが一般的である。一般にユーザはプログラムを購入する際に個人的な使用が許諾され、特に使用期限が設けられない場合もある。

【0003】 しかし、たとえば、いわゆるシェアウェアや試用プログラムのように、特定の期間無料または廉価で試用させ、その後さらに使用を希望するユーザにさらに使用許諾（ライセンス）を与える場合もある。この使用許諾に使用期限（ライセンス期間）を設ける場合も多い。

【0004】 ライセンス期間が設けられるプログラムには、ライセンスキーあるいはプロダクトキーが与えられ、正当なキーと正当な期間情報が与えられてプログラムの全ての機能が実行されるようになっているのが一般的である。すなわち、ユーザはプログラムの使用許諾元から発行された正当なキー情報を入力し、かつ、正当な期間（ライセンス期間）内での使用でなければプログラムを利用することができない。

【0005】 そこで、ライセンス期間が経過した場合、さらにプログラムの使用を希望するときには、ユーザは使用許諾元（プログラム提供者）から新たなライセンス

キーを入手する必要がある。新たなライセンスキーの入手は、一般に、メール等によるユーザからのライセンス更新申請、プログラム提供者による更新申請の認証、プログラム提供者による更新キーの発行送付、ユーザによる更新キーの適用、というステップを経る。

【0006】

【発明が解決しようとする課題】 しかしながら、前記した新たなライセンスキー（更新キー）の申請・発行・取得の手続はユーザおよびプログラム提供者の双方にとって煩雑である。すなわち、ユーザはライセンス期間内にはほとんど意識することがなかった更新手続を行う必要があり、プログラム提供者にとってはユーザからの申請に個別に対応しなければならない。さらにユーザは新たな更新キーを適用しなければならない。このような事務手続を簡略化するためにライセンス期間を相当に長くする方策も考え得るが、ライセンス期間を短くして有効に対価を回収したい場合にはその要求に反する。

【0007】 あるいは特定の会（クラブ）を結成し、この会員向けに特定のプログラムを包括的に使用許諾するような場合には、プログラムごとにライセンス更新の申請を受け付けていてはその認証事務手続が膨大になり効率化が強く要請される。

【0008】 本発明の目的は、プログラム使用許諾（ライセンス）期間の更新認証事務を効率化することにある。また、本発明の目的は、ライセンス期間を自動的に更新できる技術を提供することにある。また、本発明の目的は、ユーザおよびプログラム提供者の双方に利便性の高いライセンス更新システムを提供することにある。また、本発明の目的は、システムの利便性のみならず、セキュリティおよびフレキシビリティに優れたライセンス更新システムおよび方法を提供することにある。

【0009】

【課題を解決するための手段】 本願の発明の概略を説明すれば、以下の通りである。すなわち、本発明のプログラム使用許諾期間の更新方法は、現在日時がプログラムの使用許諾期間内であるかを判断する第1判断ステップと、第1判断ステップの判断が偽の場合、インデックス・サーバに対し、インデックス・ファイルの送信要求を発するステップと、インデックス・サーバからインデックス・ファイルを受信するステップと、インデックス・ファイルに含まれる認証サーバのアドレスに、認証要求を発するステップと、認証サーバから認証情報を受信するステップと、認証情報に認証成功の情報が含まれるかを判断する第2判断ステップと、第2判断ステップの判断が真の場合、プログラムの使用許諾期間を更新するステップと、を含む。

【0010】 なお、プログラムの起動を契機に前記第1ステップが実行され、使用許諾期間の更新の後にプログラムが実行可能となるようにしても良い。また、アドレス情報が暗号化され、この暗号化されたアドレス情報を

10

20

30

40

50

復号化するステップを有しても良い。また、認証要求には、プログラムの使用が許諾されているグループに属するか否かを判断するためのユーザ識別情報を含み、認証サーバは、このグループを管轄する者が管理するものであってもよい。さらに、認証要求を発する前に、ユーザ識別情報とパスワードとを入力するよう要求する画面を表示し、この画面にはプログラムの使用許諾条件に関する情報を表示しても良い。

【0011】本発明によれば、ライセンス期間の満了を自動的に判断して、プログラム提供者（認証サーバ）に自動的に認証要求を発する。認証結果は認証サーバからユーザに返送され、ライセンス期間が自動的に更新される。このためユーザは更新キーの発行を申請することなく、簡便にプログラムのライセンスを再度得ることができる。一方、プログラム提供者は、ユーザからの更新申請が定式化されて送付されるので認証の自動化が可能であり、また、ユーザの更新要求はインデックス・サーバを参照して行われるので認証サーバの変更を容易に行うことができる。すなわち、認証サーバを変更しても、ユーザに対するアドレス送付の必要はなく、インデックス・サーバのインデックス・ファイルを更新するのみで認証サーバのアドレスを変更できる。また、ユーザはインデックス・サーバから認証サーバのアドレス情報を取得するので、認証サーバのアドレスを公開する必要がなく認証サーバのセキュリティを向上できる。また、送付されるアドレス情報は暗号化できるのでさらにセキュリティを向上できる。

【0012】本発明は、たとえばユーザを会員とする組織にプログラムを許諾する場合に好適なものである。プログラム提供者はユーザの識別情報を会員番号として管理し、会員である限りプログラム使用のライセンスを与える場合などに適用できる。この場合、ユーザはライセンス期間の自動更新に際して会員であることの証明であるユーザ識別情報（会員番号）とパスワードを認証サーバの送信する。本発明では、このような会員番号（識別情報）の入力画面を備える。認証サーバは会員データベースを参照して有効な会員であれば認証を与える。

【0013】また、本発明は、ユーザからの要求を受取るステップと、要求の受信を契機として、ユーザが使用するプログラムの使用許諾に関する認証を与えるサーバのアドレス情報を含むインデックス・ファイルを生成または選択するステップと、インデックス・ファイルを要求を発したユーザに送信するステップと、を有するプログラムの使用許諾方法である。なお、インデックス・ファイルに含まれるアドレス情報の部分は暗号化することができる。このような方法によりユーザはインデックス・ファイルを取得できる。

【0014】なお、本発明の方法は、システムあるいはプログラムとして把握することも可能である。

【0015】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。ただし、本発明は多くの異なる態様で実施することが可能であり、本実施の形態の記載内容に限定して解釈すべきではない。なお、実施の形態の全体を通して同じ要素には同じ番号を付するものとする。

【0016】以下の実施の形態では、主に方法またはシステムについて説明するが、当業者であれば明らかとなり、本発明はコンピュータで使用可能なプログラムとしても実施できる。したがって、本発明は、ハードウェアとしての実施形態、ソフトウェアとしての実施形態またはソフトウェアとハードウェアとの組合せの実施形態をとることができる。プログラムは、ハードディスク、CD-ROM、光記憶装置または磁気記憶装置等の任意のコンピュータ可読媒体に記録できる。

【0017】また以下の実施の形態では、クライアントのシステムおよびサーバのシステムとして、一般的なコンピュータシステムを用いることができる。実施の形態で用いることができるコンピュータシステムは、中央演算処理装置（CPU）、主記憶装置（メインメモリ：RAM）、不揮発性記憶装置（ROM）、コプロセッサ、画像アクセラレータ、キャッシュメモリ、入出力制御装置（I/O）等、一般的なコンピュータシステムに備えられるハードウェア資源を備える。また、ハードディスク装置等の外部記憶装置、インターネット等のネットワークに接続可能な通信手段を備えることができる。コンピュータシステムには、パーソナルコンピュータ、ワークステーション、メインフレームコンピュータ等各種のコンピュータが含まれる。

【0018】図1は、本発明の一実施の形態であるライセンス期間の更新方法に適用できるシステムの一例を示した概念図である。本実施の形態のシステムは、インターネット1に、クライアントのコンピュータシステム2、インデックス・サーバ3、認証サーバ4が接続されている。

【0019】インターネット1は、良く知られているように、IP（Internet Protocol）に従って通信が行われる世界的に開かれたネットワークの一形態である。ここではインターネットを例示するが、他のネットワーク形態を利用することも可能である。たとえば専用電話線により接続されたネットワークあるいはCATV等のケーブルネットワークでもよい。インターネットの概念には、特定の者にのみ利用が制限されるイントラネットも含む。

【0020】クライアントのコンピュータシステム2（以下単にクライアント2という）は、プログラム提供者等によって使用許諾（ライセンス）が与えられるプログラムを使用するユーザのコンピュータシステムである。プログラムにはアプリケーション・プログラムが例示できる。以下の説明では、クライアント2として一般

的なコンピュータシステムを例示して説明するが、携帯電話6、携帯情報端末(PDA: Personal Digital Assistants)7等がクライアント2として機能してもよい。また、図1では単一のクライアント2として表現しているが、クライアント2が多数存在することは言うまでもない。

【0021】インデックス・サーバ3は、ユーザの要求に応じて、認証サーバ4のURL(uniform resource locator)を含むインデックス・ファイルをユーザに送信する機能を持つ。認証サーバ4は、ユーザからのライセンス期間更新要求に対して認証を与える機能を持つ。インデックス・サーバ3および認証サーバ4には、前記したとおり一般的なコンピュータシステムが利用できる。また、図1では各々単一のインデックス・サーバ3および認証サーバ4として表現しているが、複数のインデックス・サーバ3および認証サーバ4が存在してもよい。

【0022】図2は、本実施の形態のライセンス期間更新の概要について時系列に示した図である。時刻t0でユーザがアプリケーション・プログラムをダウンロードする場合を考える(ステップ10)。なお、ユーザはこの時点でプログラム提供者の管理するグループ(会)の会員であるとする。ダウンロードの時からアプリケーション・プログラムのライセンス期間が開始し、ライセンスは時刻t0~t2の間で有効であるとする。この期間(t0~t2)は、プログラムをインストールする際に同意したライセンス期間となる。時刻t1でユーザがアプリケーション・プログラムを起動した時、ライセンスは有効であるためアプリケーション・プログラムが実行できる(ステップ11)。

【0023】一方、ライセンス期間が時刻t2で満了した後の時刻t3にユーザがアプリケーション・プログラムを実行しようすると、従来であればライセンスが有効ではないためプログラムの実行はできない。しかし、本実施の形態では、アプリケーション・プログラムの起動を契機としてユーザの認証を自動的にを行い、ライセンス期間を自動的に更新する(ステップ12)。この場合、ユーザの会員資格は依然有効であるため認証が成功しライセンス期間が時刻t4まで更新されてアプリケーション・プログラムが実行可能になる。なお、この更新の際のライセンス期間(t3~t4)は、前記プログラムをインストールする際のライセンス期間(t0~t2)と相違しても良い。更新されたライセンス期間は、更新の際のライセンス(契約)に従う。たとえば試用目的に廉価でプログラムを頒布し、その後正式に対価を支払ってプログラムを利用するような場合、試用のライセンス期間(プログラムダウンロードの際のライセンス期間)を1ヶ月程度と短くし、正式契約(更新)の際のライセンス期間を1年程度に長くできる。

【0024】時刻t5でユーザがグループから脱会した場合(ステップ13)、ユーザが会員資格がない期間の

時刻t6でアプリケーション・プログラムを起動すると、本実施の形態のシステムは前記同様に認証確認を行うが会員資格が無効なので認証に失敗し、ライセンス期間は更新されず、結果としてアプリケーション・プログラムの実行はできない(ステップ14)。

【0025】しかしながら、ユーザが時刻t7で再度グループに入会した場合(ステップ15)、それ以降の時刻t8にユーザがアプリケーション・プログラムを実行すると、前記ステップ12の場合と同様にライセンスが有効になり、アプリケーション・プログラムが実行できるようになる(ステップ16)。すなわち、本実施の形態のシステムは会員資格が有効である限りユーザに認証が与えられてアプリケーション・プログラムが利用できるようになるシステムである。

【0026】図3は、クライアント2、インデックス・サーバ3、認証サーバ4の構成の一例を示したブロック図である。

【0027】クライアント2には、アプリケーション・プログラム20を有し、アプリケーション・プログラム20には、ライセンス期間チェックモジュール21、会員認証モジュール22、アプリケーション実行モジュール23を有する。また、クライアント2には時計24を有する。

【0028】アプリケーション・プログラム20は、プログラム提供者から提供されるプログラムである。なお、ここではアプリケーション・プログラムを例示するが、プログラム提供者から提供されるプログラムはアプリケーション・プログラムには限られない。たとえば特定のシステムで稼動するシステムプログラム、特定のアプリケーションで利用可能なマクロプログラム等であってもよい。

【0029】ライセンス期間チェックモジュール21は、アプリケーション・プログラムの起動に際して起動され、現在時刻がライセンス期間内にあるかを判断する機能を持つ。現在時刻は時計24から取得できる。なお、ライセンス期間の情報はクライアント2のシステムの何れかの記憶領域に記録されるほか、適当な通信回線で接続されている他のシステムに記録されても良い。この場合、多数のユーザのライセンス期間を一元的に管理できる。またこの場合、ライセンス期間チェックモジュール21は、このような通信機能をも有し、適切な情報を取得する手段を有する。

【0030】会員認証モジュール22は、インデックス・サーバ接続手段221、インデックス・ファイル取得手段222、取得情報デコード223、UID/PWD取得・新ライセンス表示ダイアログ224、認証サーバ接続手段225、認証結果取得手段226、認証結果チェック手段227を有する。

【0031】インデックス・サーバ接続手段221は、インデックス・サーバ3に対しインデックス・ファイル

10

20

30

40

50

を取得するよう要求を発する。なお、この要求には適切なインデックス・ファイルを選択するために必要な情報、たとえばアプリケーション・プログラムのプロダクトナンバー等を含めることができる。

【0032】インデックス・ファイル取得手段222は、インデックス・サーバ3から送信されたインデックス・ファイルを受信する、取得情報デコーダ223は、受信したインデックス・ファイルに含まれる暗号を復号化する。本実施の形態では、インデックス・ファイルが暗号化できるため、システムのセキュリティ、特に認証サーバ4のアドレス情報に対するセキュリティを向上できる。

【0033】UID/PWD取得・新ライセンス表示ダイアログ224は、認証サーバ4に認証要求を行う際に必要な会員番号等のユーザ識別情報およびパスワードを取得する機能を持つ。また、認証後に付与されることとなる新ライセンスの契約内容を表示する機能を持つ。新ライセンス（契約）文書は、インデックス・ファイルに含めてインデックス・サーバ3から送ることにより、ライセンス更新ごとに新しい内容を表示できる。

【0034】認証サーバ接続手段225は認証サーバ4への認証要求を発する機能を持つ。認証要求には、前記したユーザ識別情報（UID）とパスワード（PWD）を含めることができる。認証結果取得手段226は、認証サーバ4から送信された認証結果を取得する。認証結果チェック手段227は、取得した認証結果をチェックし、認証成功の場合にはライセンス期間を更新してアプリケーション・プログラムの実行を可能にする。アプリケーション実行モジュール23は、アプリケーション・プログラムを実行する。

【0035】インデックス・サーバ3には、インデックス選択・送信手段31とインデックス32を含む。インデックス選択・送信手段31はクライアント2からのインデックス・ファイル送信要求を受けて、インデックス32から適切なインデックス・ファイルを選択し、あるいは適切なインデックス・ファイルを生成して、クライアント2にそのインデックス・ファイルを送信する。なお、インデックス・ファイルはユーザごとあるいはアプリケーション・プログラムごとに予め作成し、インデックス32に記録することが好ましい。インデックスの選択あるいは生成には、ユーザからの送信要求に含まれるアプリケーション・プログラムの製造番号あるいはユーザ番号を参照できる。

【0036】認証サーバ4には、認証データ取得手段41、認証可否判断手段42、認証結果送信手段43、会員データベース44を含む。認証データ取得手段41は、クライアント2からの認証要求とそれに含まれる認証データ（UIDおよびPWD）を受取る。なお、認証データにはUIDおよびPWD以外のデータが含まれても良い。認証可否判断手段42は認証データに基づいて

認証の可否判断を行う。判断には会員データベース44を参照する。たとえば会員データベース44には現在有効な会員をそのUIDとPWDとでデータベース化し、ユーザから送付された、UIDおよびPWDと一致するか否かを判断して行える。なお、会員データベース44は認証サーバ4内に有する必要はなく、他のシステムに記録されていてもよい。認証結果送信手段43は、認証可否判断手段42で判断した認証結果をクライアント2に送信する。

【0037】図4は、本実施の形態のライセンス期間の更新方法の一例を示したフローチャートである。ステップ50のアプリケーション・プログラムの起動から説明を開始する。

【0038】アプリケーション・プログラムが起動されると、プログラムはライセンス期間と現在日時を取得し（ステップ51）、現在日時がライセンス期間内であるかを判断する（ステップ52）。ライセンス期間である場合は、ステップ72に進んでアプリケーション・プログラムを実行する（ステップ72）。この場合、ライセンスは有効なので本実施の形態の会員認証は行われず、速やかにアプリケーション・プログラムが実行される。

【0039】ライセンス期間外である場合、ライセンスは現在無効であるため、会員認証モジュール22を起動する（ステップ53）。会員認証モジュールが起動されると、モジュールはインデックス・ファイル取得要求をインデックス・サーバ3に対して発する（ステップ54）。

【0040】インデックス・サーバ3は、ユーザからのこの要求を受取り（ステップ55）、この要求受信を契機としてインデックス・ファイルの選択または生成を行う（ステップ56）。インデックス・ファイルの選択または生成にはインデックス32を参照する。インデックス・サーバはこの段階でインデックス・ファイルを暗号化しても良い。暗号化は予め行い、インデックス32に暗号化インデックス・ファイルを記録しておくことが好ましい。その後、インデックス・サーバ3は暗号化されたインデックス・ファイルをクライアント2に送信する（ステップ57）。

【0041】インデックス・ファイルには前記したように認証サーバ4のURLを含む。このようにユーザはインデックス・サーバ3を参照して認証サーバ4のURLを取得するので、認証サーバ4のURLを認証サーバ4によって公開する必要がない。また、クライアント2は本実施の形態の会員認証モジュールを用いる限りインデックス・サーバ3にアクセスすれば、常に最新の認証サーバ4のURLが取得できる。このため、認証サーバ4のURLに変更があってもユーザは無関心でよい。また、認証サーバ側ではURLを変更してもインデックス・サーバ3のインデックス・ファイルを変更するだけでよく、各ユーザへの周知あるいは連絡の必要がない。

【0042】また、インデックス・ファイルは暗号化されるのでシステムのセキュリティ、特に認証サーバ4のアドレスに対するセキュリティを向上できる。なお、インデックス・ファイルには、認証サーバ4のURLのほかにライセンス期間やプログラム使用条件等の情報を含めることができる。

【0043】図5はインデックス・サーバ3が送信するインデックス・ファイルの一例を示す図である。本ファイルはXML (extensible markup language) で記述されている。ここでは「url」タグで囲まれた部分に認証サーバ4のURLが暗号化されて記述されている。また、「information」タグで囲まれた部分には、「frequency」タグで囲まれているライセンス期間、「requirement」タグで囲まれたプログラム使用条件に関するテキストが記述されている。

【0044】次に、クライアント2が暗号化されたインデックス・ファイルを受信すると(ステップ58)、この暗号を復号化し平文のインデックス・ファイルを得る(ステップ59)。図6は復号化した後のインデックス・ファイルの一例を示す。図5と比較して「url」タグで囲まれた部分が意味のある平文になっている。

【0045】なお、ここではインデックス・ファイルの一部が暗号化・復号化される例を示しているが、インデックス・ファイルの全てが暗号化されても良いことは勿論である。

【0046】次に、クライアント2は、UID (会員番号) とPWD (パスワード) を入力する画面を表示する(ステップ60)。また、この画面にはプログラム使用条件が同時に表示されても良い。

【0047】図7は、会員番号およびパスワードを入力する画面の一例を示した図である。画面のウィンドウ80内には、会員番号を入力するフィールド81とパスワードを入力するフィールド82を有する。また、サブウィンドウ83にはプログラム使用条件が表示される。この新しいプログラム使用条件にユーザが同意する時には「はい」のボタン84をクリックし、同意しない時には「いいえ」のボタン85をクリックする。なお、「いいえ」のボタン85が押された時にはプログラムは終了する。

【0048】次に、クライアント2は、たとえば前記フィールド81、82に入力されたデータからUIDとPWDを取得し(ステップ61)、これらデータを認証データとする。なお、ここではユーザ入力により認証データを得る方法を例示したが、たとえばクライアント2のシステム内にユーザ情報を記録し、このユーザ情報から必要なデータを取得して認証データとしても良い。

【0049】次に、クライアント2は、認証サーバ4に認証の取得要求を発する(ステップ62)。取得要求には前記ステップで取得したUID/PWD等の認証データを含める。

【0050】次に、認証サーバ4がクライアント2からの認証要求を受取り、同時に認証データを受取る(ステップ63)。認証サーバ4は、クライアントからの要求を契機として、会員データベース44を検索し(ステップ64)、認証要求の会員の資格が有効であるかを判断する(ステップ65)。会員資格が有効である時には、認証成功の「ReturnValue」を生成し(ステップ66)、会員資格が無効の場合には認証失敗の「ReturnValue」を生成する(ステップ67)。そしてこの「ReturnValue」を認証結果としてクライアント2に送信する。

【0051】クライアント2は、「ReturnValue」を受信し(ステップ69)、「ReturnValue」が認証成功であるかを判断する(ステップ70)。認証成功の場合、ライセンス期間を新たなライセンス期間に更新し(ステップ71)、アプリケーション・プログラムを実行する(ステップ72)。その後処理を終了する(ステップ73)。認証失敗の場合はライセンス期間を更新することなく、また、アプリケーション・プログラムを実行することなく終了する(ステップ73)。

【0052】本実施の形態によれば、ユーザはライセンス期間を経過したプログラムを実行するに際して、プログラム提供者に新たなライセンスの申請、ライセンス期間の更新申請を行う必要がない。本実施の形態では、ライセンス期間の経過を自動的に判断し、認証を自動的に取得できる(ただしユーザID(会員番号)とパスワードの入力は要求される)。また、本実施の形態によれば、認証サーバ4のアドレスをインデックス・サーバ3から取得するので、認証サーバ4のアドレス変更を容易に行える。また、インデックス・ファイルを認証ごとに取得するので、最新の使用条件等、最新データをユーザに提示できる。さらにインデックス・ファイルを暗号化してシステムのセキュリティを向上できる。

【0053】以上、本発明者によってなされた発明を発明の実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更することが可能である。

【0054】たとえば、前記実施の形態では、プログラム使用の当初からライセンスを与えられている場合を説明したが、当初は試用段階のライセンスが与えられ、その後正式なライセンスが与えられる場合にも適用できる。

【0055】また、前記実施の形態では、認証サーバ4が単一の場合を説明したが、図8に示すように複数の認証サーバ4-1、4-2を有しても良い。ユーザに異なるプログラム提供者からのプログラムが提供されている時には、提供者ごとに認証サーバを設置し、提供者独自のユーザ(会員)管理を行う場合にも本発明が利用できる。この場合、プログラム提供者が異なっても、図示するように単一のインデックス・サーバを共用することができる。

【0056】また、図9に示すように、インデックス・サーバと認証サーバを単一のサーバで実現しても構わない。

【0057】さらに、本発明はライセンス期間を自由に設定できる。そしてライセンス期間の更新が簡便に実現できる本発明は、そのようなライセンス期間を自由に設定したいと望むプログラム提供者やユーザに安全で且つ利便性の高いシステムを提供できるものである。

【0058】また、前記実施の形態ではインデックス・ファイルの一部または全部が暗号化される例を示したが、インデックス・ファイルは暗号化されなくても良い。

【0059】

【発明の効果】本願で開示される発明のうち、代表的なものによって得られる効果は、以下の通りである。すなわち、プログラム使用許諾（ライセンス）期間の更新認証事務を効率化することができる。また、ライセンス期間を自動的に更新でき、ユーザおよびプログラム提供者の双方に利便性の高いシステムを提供できる。また、セキュリティおよびフレキシビリティに優れたライセンス更新システムおよび方法を提供できる。

【図面の簡単な説明】

【図1】本発明の一実施の形態であるライセンス期間の更新方法に適用できるシステムの一例を示した概念図である。

【図2】本発明の一実施の形態であるライセンス期間更新の概要について時系列に示した図である。

【図3】クライアント、インデックス・サーバ、認証サーバの構成の一例を示したブロック図である。

【図4】本発明の一実施の形態であるライセンス期間の更新方法の一例を示したフローチャートである。

【図5】インデックス・サーバが送信するインデックス・ファイルの一例を示す図である。

【図6】復号化した後のインデックス・ファイルの一例を示す図である。

【図7】会員番号およびパスワードを入力する画面の一例を示した図である。

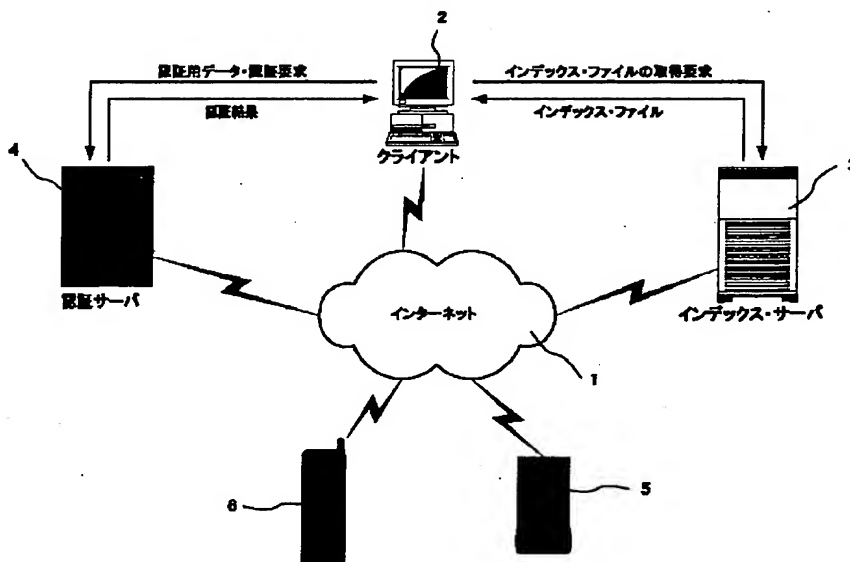
【図8】本発明の他の実施の形態の一例を示したブロック図である。

【図9】本発明の他の実施の形態の他の例を示したブロック図である。

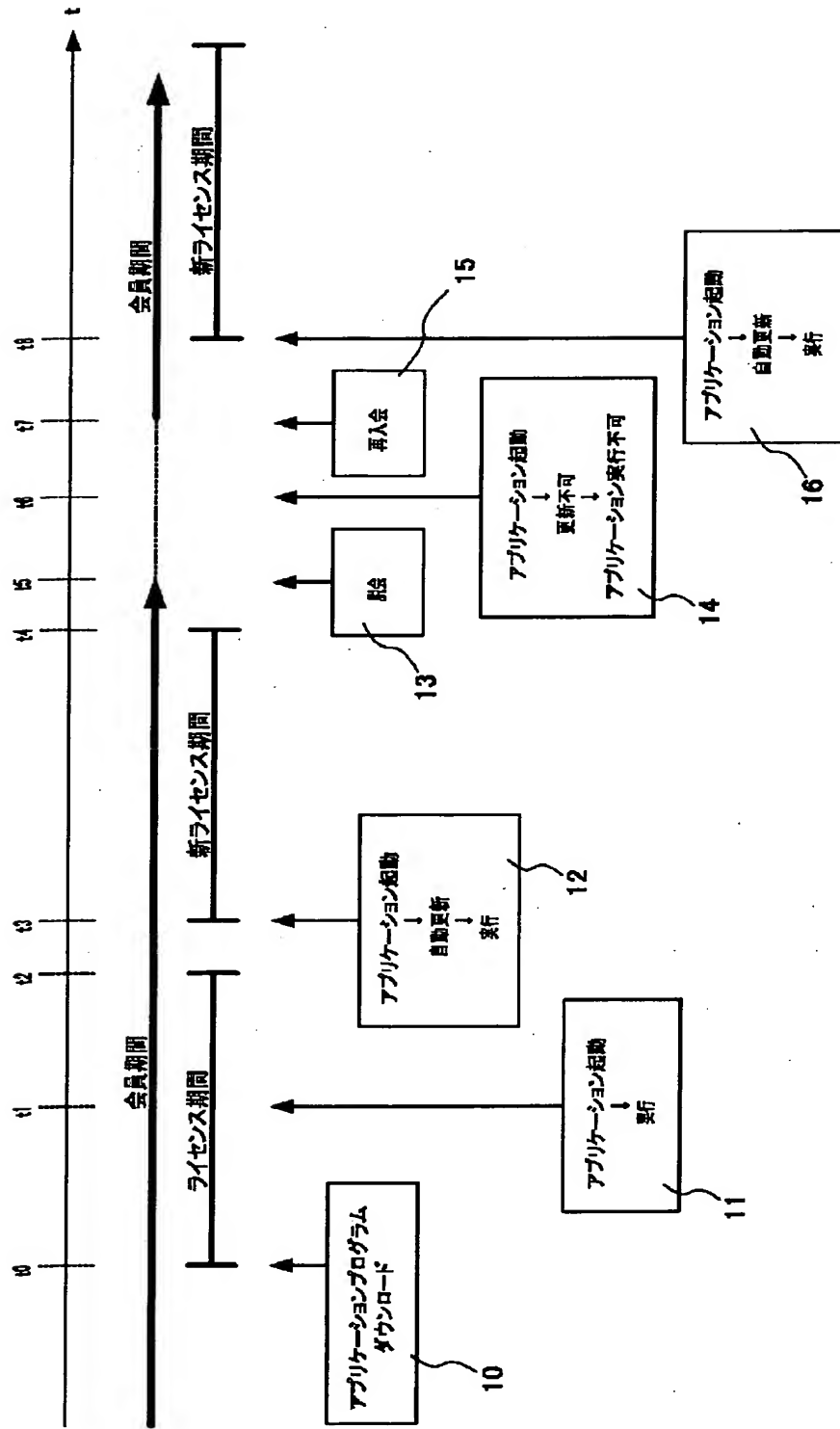
【符号の説明】

1…インターネット、2…クライアント、3…インデックス・サーバ、4…認証サーバ、5…携帯情報端末（PDA）、6…携帯電話、20…アプリケーション・プログラム、21…ライセンス期間チェックモジュール、22…会員認証モジュール、221…インデックス・サーバ接続手段、222…インデックス・ファイル取得手段、223…取得情報デコード、224…UID/PW D取得・新ライセンス表示ダイアログ、225…認証サーバ接続手段、226…認証結果取得手段、227…認証結果チェック手段、23…アプリケーション実行モジュール、24…時計、31…インデックス選択・送信手段、32…インデックス、41…認証データ取得手段、42…認証可否判断手段、43…認証結果送信手段、44…会員データベース、80…ウィンドウ、81、82…フィールド、83…サブウィンドウ、84、85…ボタン、t0～t8…時刻。

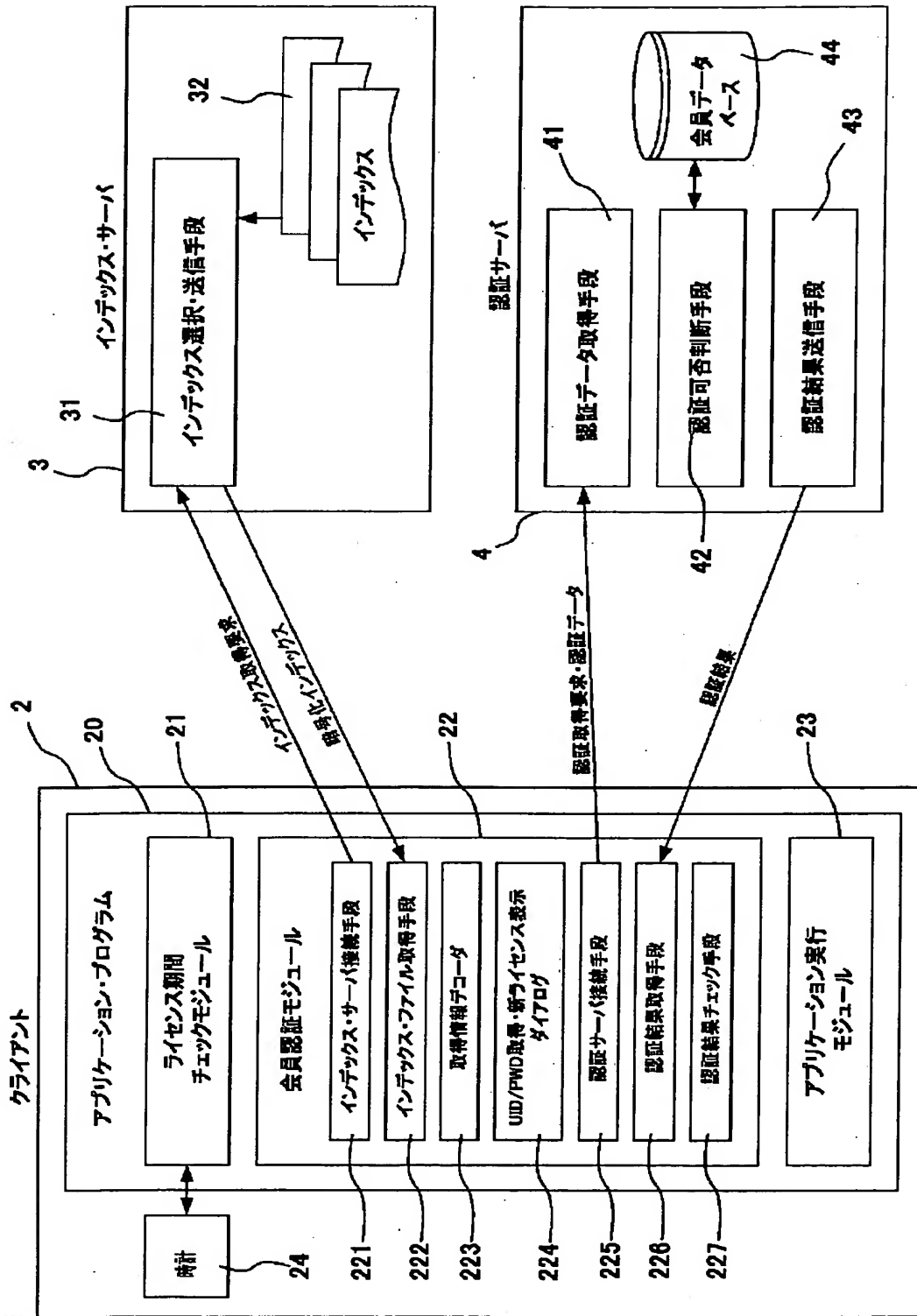
【図1】



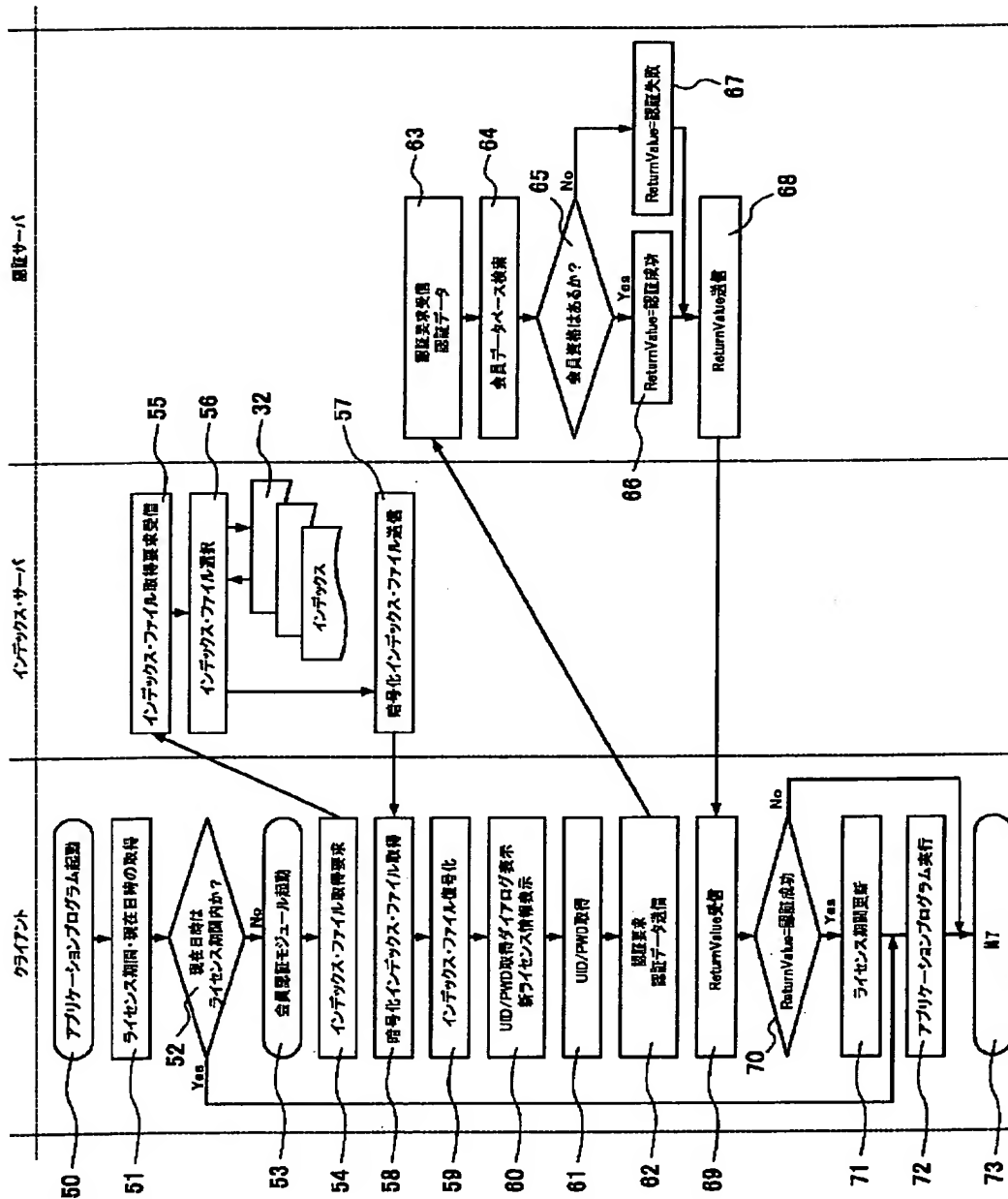
【図2】



【図3】



【図4】



【図5】

```

<?xml version="1.0" encoding="SHIFT_JIS" ?>
<pkm-taxonomy version="1.0" local save="no">
<description>user authentication server</description>
<site>
<url>aabbbcccdseiiiissel#$$$&&&.....
.....aashhhjjjddkkifir</url>
<information>
<frequency>385</frequency>
<requirement>プログラム使用許諾条件
このプログラムは以下の条件に従うことを.....
</requirement>
</information>
</site>
</pkm-taxonomy>

```

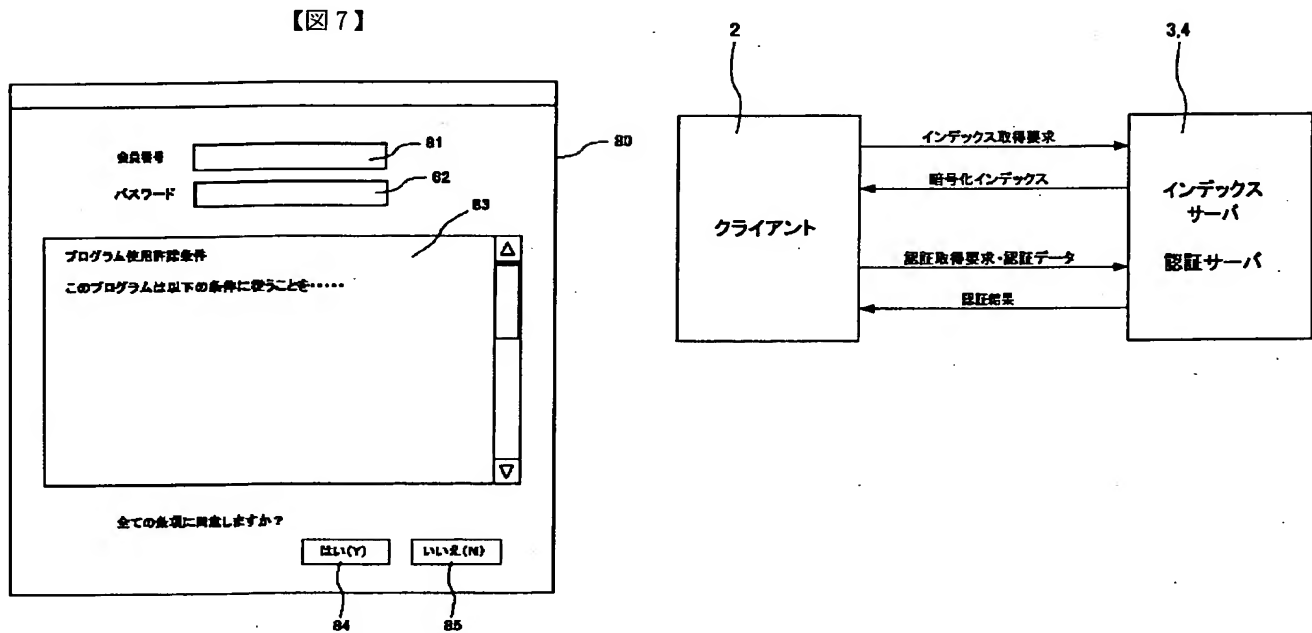
【図6】

```

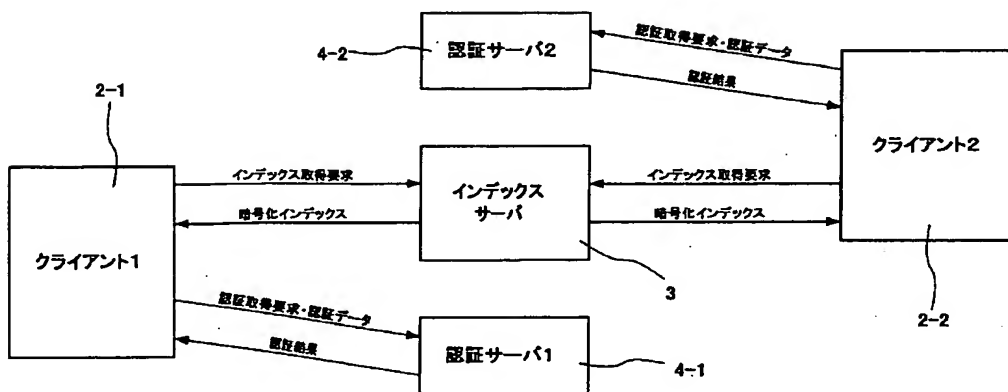
<?xml version="1.0" encoding="SHIFT_JIS" ?>
<pkm-taxonomy version="1.0" local save="no">
<description>user authentication server</description>
<site>
<url>https://www.abcd.com/cgi-bin/abc_club/index.cgi?html=index.html</url>
<information>
<frequency>385</frequency>
<requirement>プログラム使用許諾条件
このプログラムは以下の条件に従うことを.....
</requirement>
</information>
</site>
</pkm-taxonomy>

```

【図9】



【図8】



フロントページの続き

(72)発明者 川口 佳文

神奈川県大和市下鶴間1623番地14 日本ア
イ・ビー・エム株式会社 大和事業所内

(72)発明者 中垣 勝博

東京都港区六本木三丁目2番12号 日本ア
イ・ビー・エム株式会社内

Fターム(参考) 5B076 FA00 FB01 FB11